



# **OCNUS NAVY ENTERPRISE NETWORK (ONE-NET)**

★ Mission ★ People ★ Capability

## **Outlook Web Access User Training**

**December 2007**



# ***Your Responsibility***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **It is your responsibility as a Government representative to protect the DoD information that is entrusted to you.**
- ▶ **By using your home computer for OWA access you are expanding the Global Information Grid (GIG)**
- ▶ **Any vulnerabilities on your current system are now added to the GIG.**
- ▶ **The more secure your computer is, the less risk is added to the GIG.**



# ***Accessing OWA from Home***



★ Mission ★ People ★ Capability

► **In order to access your ONE-NET email account via OWA you will need the following items:**

1. A CAC with valid PKI certificates
2. CAC reader and drivers
3. Middleware (CAC software)
4. PKI Installroot software
5. Anti-virus software
6. Firewall software



# Common Access Cards (CAC)



★ Mission ★ People ★ Capability

## ► The Common Access Card (CAC).

- If your CAC does not have all three certificates (identity, e-mail signature, and e-mail encryption) go through the normal process at your command to update your CAC at the RAPIDS/DEERS facility.
- If your CAC is expired, contact your command Trusted Agent (TA).



# CAC Readers



★ Mission ★ People ★ Capability

- ▶ **CAC readers and software are available for command-authorized OWA users from their parent command.**
- ▶ **Commands can acquire CAC readers/software via Internet, local computer stores, or GSA.**
- ▶ **USB and PCMCIA personal CAC readers may also be purchased online.**
  - Internet Search for "Purchase CAC reader"



# CAC Software



★ Mission ★ People ★ Capability

▶ **Unless you have personally purchased them, the CAC Reader and software license to operate the CAC reader are the property of the Navy. At the termination of your employment:**

- Remove the CAC reader software from your home computer.
- Return all Government owned property to your Command.

▶ **Personal copies of ActivClient software may also be purchased online:**

- [http://www.actividentity.com/products/activclient\\_family\\_home.php](http://www.actividentity.com/products/activclient_family_home.php)
- ActivClient CAC 6.1 or above must be installed on the PC



# PKI INSTALLROOT UTILITY



★ Mission ★ People ★ Capability

- ▶ In addition to ActivCard software you must also go to the Navy's INFOSEC web site <https://infosec.navy.mil/> and download the most current version of the PKI INSTALLROOT utility (left column on home page under PKI). (As of December 2007, ver 2.19a)

- **NOTE:** You will need a CAC card to access this site

- ▶ Running the utility will install all the DOD root certifications (CA-5, CA-6, etc) onto your computer and create the "*trusted*" chain that will allow their CAC certificates to show up in the authentication box when accessing OWA.



# Outlook Web Access (OWA)



★ Mission ★ People ★ Capability

- ▶ Outlook Web Access (OWA) is a convenience that allows access to e-mail from outside the DoD network.
- ▶ For all DoD, OWA is required to use CAC identity certificates for authentication, email signing and encryption.
- ▶ To access OWA from your Non-DoD computer you must install the CAC reader, CAC reader drivers, CAC middleware (software), anti-virus & Spyware protection and personal firewall software.
  - **Important Note**: The ONE-NET Service Desk is **not** responsible for set-up or problems with non-DOD assets!





# OWA Access



★ Mission ★ People ★ Capability

- ▶ **Network access via OWA to your e-mail is a privilege not a right.**
- ▶ **If you do not protect your home computer, you are not protecting the GIG.**
- ▶ **A user configured password-protected screen-lock will be set to activate with 15 minutes of inactivity (see slide for setting this option).**



# ***What is Spyware***



★ Mission ★ People ★ Capability

- ▶ **Spyware is a malicious program that aids in gathering information about a person or organization without their knowledge.**
- ▶ **Spyware can get in a computer by web browsing, viewing an HTML email, opening an attachment, or running an executable file.**



# ***How to avoid Spyware***



★ Mission ★ People ★ Capability

- ▶ **Be suspicious of any email from people you do not know.**
- ▶ **Don't open attachments that you are not expecting.**
- ▶ **Even if you know the sender, if an unexpected or unusual email is unsigned or unencrypted verify that the email and attachment are valid prior to opening it. Do this by calling or emailing the individual.**



# ***If you think you have Spyware***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **Run an immediate virus scan of your computer with the latest signature update.**
- ▶ **Both Symantec and MacAfee virus scan software contain the ability to detect Spyware.**



# ***Basic Security principles***

★ Mission ★ People ★ Capability

- ▶ **Use anti-virus software on your personal computer and update the signature at least weekly.**
- ▶ **Scan all files and email downloaded from the Internet**
- ▶ **Download operating system, application and web browser software patches and updates automatically.**
- ▶ **Install and use a personal firewall when connected to the Internet**



# ***Basic Security principles***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **Backup Important files**
- ▶ **Use complex passwords at home, not just on DoD systems.**
- ▶ **Disconnect the computer from the internet when not on-line.**
  - Leaving your computer connected for extended periods of time leaves an opportunity that a hacker can use to access your computer.
  - Leaving an OWA session connected unnecessarily, increases the risk to the GIG.



# ***Basic Security principles***

★ *Mission* ★ *People* ★ *Capability*

- ▶ **Use only a wired internet connection (i. e., Phone dial-up, cable or DSL modem).**
- ▶ **Ensure that no wireless connection is turned on during the duration of the OWA session.**
  - Wireless device on computer accessing OWA should either be removed or disabled
  - Wireless Access Point(s) on the same internet connection as the computer accessing OWA should be powered off
- ▶ **Ensure that no other web browser connections are opened for the duration of the session.**



# ***Basic Security principles***



★ Mission ★ People ★ Capability

- ▶ **Clear your cache before logging off. (see slide regarding this operation)**
- ▶ **No peer-to-peer file-sharing software (examples are Skype, Kazaa, Morpheus, and Limewire) may be installed on your system.**
- ▶ **At the end of your session, log off and either reboot or shut down your computer.**





# Screen Saver



★ Mission ★ People ★ Capability

▶ The Screen saver must be set to lock after 15 minutes.

1. Go to **Start, Settings, Control panel**

2. Click on **Display**

3. Click on **Screensaver**

4. Set the timer to **15** minutes

5. Click **OK**



# Clearing Data



★ Mission ★ People ★ Capability

- ▶ **Clearing.** Removal of data from an information system, its storage devices, and other peripheral devices with storage capacity, in such a way that the data may not be reconstructed using common system capabilities
- ▶ When you delete files from a disk on your computer, Windows does not erase the contents of the files from the disk, it only deletes “references” to these files from the systems tables.
- ▶ The contents of the files remain on the disk and can be recovered using any recovery utility.



# ***Handling of Government Information***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **All DON policies and instructions are to be followed to their full extent.**
- ▶ **Same policies and procedures apply as if you were at your command.**
- ▶ **Handle, store, maintain and destroy all classified information in accordance with DoD and DON policy.**
- ▶ **Immediately notify your command of any information loss, theft or suspicious behavior of your system.**



# ***Handling of Government Information***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **Sensitive Information includes For Official Use Only (FOUO) and the Controlled Unclassified Information (CUI) data.**
- ▶ **Do not download any sensitive data to your non-DoD system.**
- ▶ **Do not process or leave sensitive data on your system.**
- ▶ **If you inadvertently saved any sensitive data to your computer contact your Command Security Manager and IAM. If possible, overwrite the file(s) using a utility provided with the anti-virus application. As a minimum, delete the file(s) and empty the Recycle Bin.**



# ***Handling of Government Information***



★ Mission ★ People ★ Capability

- ▶ **As a government OWA user you agree to unlimited government monitoring of your email account either at work or at home.**
- ▶ **Any violation may result in disciplinary action.**



# ***Accidental PII disclosure***



★ Mission ★ People ★ Capability

- ▶ **No Personal Identifiable Information (PII) information is allowed to be processed on a non DoD computer (other than PII of the OWA user).**
- ▶ **If PII data is accidentally viewed or downloaded contact your Command IAM or Security Manager within one hour.**



# ***Accidental PII disclosure***



★ Mission ★ People ★ Capability

- ▶ **If PII data is inadvertently placed on to a non DoD system, it can be removed (wiped) in two ways:**
  - 1. Delete the file from the system then clear the unused portion of the storage media using a “shredder” utility such as BC Wipe**
  - 2. Use a “shredder” utility that will completely overwrite the file from the storage media (such as “shredder” from McAfee).**



# ***Electronic Spillage***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **Electronic Spillage is data placed on an information technology system possessing insufficient information security controls to protect the data at the required classification (e.g., such as Unclassified Naval Nuclear propulsion information (U-NNPI), confidential, secret)**
- ▶ **Electronic Spillage may result in the confiscation and loss of your personal hard drive or storage media.**





# ***Electronic Spillage***



★ Mission ★ People ★ Capability

- ▶ **If an Electronic Spillage occurs on a non-DoD computer, the User is responsible to**
  - Stop processing and exit out of OWA.
  - Turn the computer off.
  - Report the incident to the Command IAM within one hour
  - Do not turn the computer on until directed by the IAM.
  - The IAM will follow the steps in NTD 03-06



# Overwriting Utilities



★ Mission ★ People ★ Capability

- ▶ **OWA User should familiarize himself/herself with the overwrite utility if provided with the security suite on their computer (e.g. McAfee shredder)**
- ▶ **BC wipe may be downloaded for non-commercial and non-government evaluation purposes only from the following web site: <http://www.jetico.com/index.htm#/bcwipe.htm>.**
- ▶ **Commands should have licensed copies of overwrite utilities available for the IAM, IAO and system administrators to clean-up electronic spillage.**



# Anti-Virus



★ Mission ★ People ★ Capability

- ▶ **In order to gain access to your ONE-NET OWA account from your home PC, you are required to install and use anti-virus protection and personal firewall software.**
- ▶ **It is your responsibility to:**
  - install anti-virus software
  - configure anti-virus software
  - perform anti-virus scans at least weekly
  - maintain anti-virus signatures up to date



# Anti-Virus



★ Mission ★ People ★ Capability

- ▶ **Anti-Virus software must be installed on your computer in order to access your ONE-NET OWA email account.**
- ▶ **Anti-Virus software can be downloaded for free by Government employees and transferred to your home computer.**
- ▶ **If you have anti-virus software running, verify that you are running a product listed at the following site: ([https://www.jtfgno.mil/antivirus/av\\_info.htm](https://www.jtfgno.mil/antivirus/av_info.htm) )**
  - **NOTE:** You will need a CAC card to access this site



# Anti-Virus



★ Mission ★ People ★ Capability

- ▶ **Update your current anti-virus signature files by downloading the updates at least weekly and when prompted. Recommend enabling the auto-update capability set to update signatures at least weekly.**
- ▶ **Scan for viruses weekly. Recommend enabling automatic virus scans to occur at least weekly, but daily is recommended.**



# ***Anti-Virus downloads***



★ Mission ★ People ★ Capability

- ▶ **Symantec Anti-virus client can be downloaded from**  
[https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc\\_nortonsw.html](https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc_nortonsw.html)
- ▶ **MacAfee can be downloaded from:** [https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc\\_mcafeesw.html](https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc_mcafeesw.html)
- ▶ **Trend Micros can be downloaded from:**  
[https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc\\_trendmicrosw.html](https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc_trendmicrosw.html)
- ▶ **Installation guides are available at the same locations as the software.**
- ▶ **These manuals should be read prior to attempted installation of the anti-virus software**



# Firewall



★ Mission ★ People ★ Capability

- ▶ **A personal Firewall is required on the computer accessing a DoD network via OWA.**
- ▶ **Protects your computer from network/hacker attacks.**
- ▶ **Must contain “Port/Protocol” Filtering.**
- ▶ **Must be configured to “deny all”, allow by exception.**
- ▶ **Approved software is available to all DoD employees at no cost from the DoD INFOSEC web (bundled with the anti-virus software).**



# ***Personal Firewall downloads***



★ Mission ★ People ★ Capability

- ▶ **Symantec Firewall is bundled with the anti-virus software can be downloaded at [https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc\\_nortonsw.html](https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc_nortonsw.html)**
- ▶ **McAfee desktop firewall can be downloaded from: [https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc\\_mcafeesw.html](https://infosec.navy.mil/ps/?t=av/av.tag&bc=av/bc_mcafeesw.html)**





# ***End your E-mail session***



★ Mission ★ People ★ Capability

## ▶ **End your e-mail session by performing the following steps:**

1. Close all web e-mail files.
2. Clear the web browser cache
3. Exit and close the browser.
4. Immediately turn off the computer. Sleep and stand-by modes are **not** acceptable.



# ***What is the cache?***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **A cache is a place where your computer stores information temporarily. The files you automatically request by looking at a Web page are stored on your hard disk in a cache subdirectory under the directory for your browser (for example, Internet Explorer).**
- ▶ **When you return to a page you recently viewed, the browser can get it from the cache rather than the original server, saving you time and the network the burden of some additional traffic.**



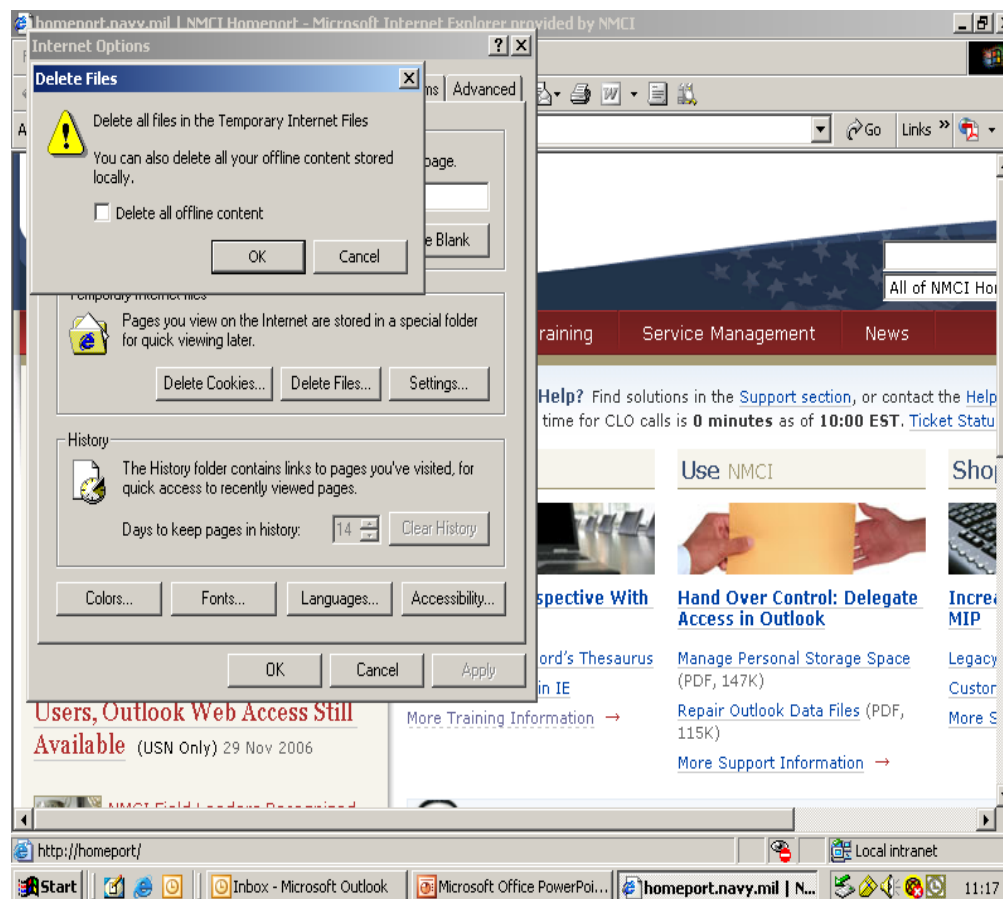
# Clear the Cache



★ Mission ★ People ★ Capability

## ► Internet Explorer

1. Open the **Tools** menu and choose **Internet Options**
2. On the **General** tab, click on **Delete Files...** under **Temporary Internet Files**
3. Click **OK**





# Clear the Cache



★ Mission ★ People ★ Capability

- ▶ Mozilla Firefox
  1. Select **Tools**
  2. **Clear Private Data**
- ▶ Automatic Clearing
  1. Select **Tools**
  2. **Options**
  3. **Privacy** tab
  4. Check in the box "Always clear my private data when I close Firefox"



# Clear the Cache



★ Mission ★ People ★ Capability

## ► Netscape

1. Open the edit menu and choose **Preferences**.
2. Click the **Advanced** Category.
3. Click on the **Cache** Category.
4. Click on the **Clear disk cache** button.
5. Click on the **Clear memory cache** button.
6. Click **OK**.



# ***Close all email files***



★ *Mission* ★ *People* ★ *Capability*

- ▶ **All email files are closed to avoid the possibility of inadvertently saving these files to your hard disk.**
- ▶ **Prevents unauthorized users, from viewing or copying this information.**



# ***Sleep/standby mode***



★ Mission ★ People ★ Capability

- ▶ **When a computer goes into sleep or standby mode, it shuts down the screen and disk drive.**
- ▶ **Once awakened, the computer returns to its former operating status. Sleep mode is used by the computer to save energy during long periods of inactivity.**
- ▶ **All information from previous sessions is still in cache and memory.**



# ***Turn off computer***



★ Mission ★ People ★ Capability

- ▶ **By turning off the computer you are clearing the memory of any residual data that may remain from your session.**
- ▶ **Clears any other temporary storage devices that may be contained in your machine.**
- ▶ **Prevents hackers from attempting to access your computer**





# Conclusion



★ Mission ★ People ★ Capability

- ▶ **ONE-NET users can find further information concerning Outlook Web Access on the ONE-NET (TBD) web-site or their local IAM.**
- ▶ **Information is available on the INFOSEC web site (under Documentation tab, NETWARCOM)**

<https://infosec.navy.mil/docs/index.jsp?tab=7&folder=166>



# Question 1



★ Mission ★ People ★ Capability

**1. In accordance with the statement of responsibility, it is acceptable for other LAN or wireless connections to exist during your ONE-NET OWA session.**

**A) True**

**B) False**



# Question 2



★ Mission ★ People ★ Capability

**2. PKI certificates are your responsibility and may be obtained from?**

- A) Your Commanding Officer**
- B) ONE-NET Service Desk**
- C) A DEERS/RAPIDS Facility**
- D) The internet**



# Question 3



★ Mission ★ People ★ Capability

**3. If your computer is lost or stolen you must notify the ONE-NET Service Desk and your IAM immediately.**

**A) True**

**B) False**



# Question 4



★ Mission ★ People ★ Capability

**4. After you have finished accessing your ONE-NET account you must turn off your computer.**

**A) True**

**B) False**



# Question 5



★ Mission ★ People ★ Capability

**5. If you are connecting to ONE-NET from your home network, you must terminate all connections except the one to ONE-NET during your session.**

**A) True**

**B) False**



# Question 6



★ Mission ★ People ★ Capability

**6. If you do not have up to date anti-virus software installed on your computer you can still access your e-mail account.**

**A) True**

**B) False**



# Question 7



★ Mission ★ People ★ Capability

**7. All classified spillage must be reported to the ONE-NET Service Desk and your IAM immediately and may subject your PC and connected storage media to confiscation.**

**A) True**

**B) False**





# Question 8



★ Mission ★ People ★ Capability

**8. If you are logged in using a DSL or cable connection, you do not have to clear your cache at the end of your session.**

**A) True**

**B) False**



# Question 9



★ Mission ★ People ★ Capability

**9. When ending your OWA session, it is acceptable to log off your computer and leave it in standby mode.**

**A) True**

**B) False**



# Question 10



★ Mission ★ People ★ Capability

**10. When ending your OWA session, which action is acceptable?**

- A) Leave your computer in sleep mode.**
- B) Leave your e-mail files open.**
- C) Leaving your computer in standby mode**
- D) Immediately turning off your computer**



# Answers



★ Mission ★ People ★ Capability

1. False
2. C) DEERS/RAPIDS Facility
3. False
4. True
5. True
6. False
7. True
8. False
9. False
- 10.D) Immediately turning off your computer



★ Mission ★ People ★ Capability